AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPELLANT:	Frank Reisinger	CONFIRMATION NO. 4346
SERIAL NO.:	09/340,782	GROUP ART UNIT: 3621
FILED:	June 28, 1999	EXAMINER: Christine O. Sherr
TITLE:	"METHOD FOR THE DEPENDABLE TRANSMISSION SERVICE DATA TO A TERMINAL EQUIPMENT AND ARRANGEMENT FOR IMPLEMENTING THE METHOD"	

MAIL STOP APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

SUBMISSION OF APPELLANT'S APPEAL BRIEF

S I R:

Pursuant to 37 C.F.R. §41.37, Appellant herewith submits his main brief in the appeal of the above-referenced application. The present Appeal is a reinstatement of a previous Appeal, in which a Brief was filed on March 10, 2003, accompanied by a check for the then-applicable fee in the amount of $320.00. In accordance with the provisions of MPEP 1204.01, this previously-paid fee is applicable to the present Appeal, and therefore the present Appeal Brief is accompanied by a check in the amount of $180.00, to pay for the balance between the previously applicable fee of $320.00 and the now-applicable of $500.00.

Submitted by,

Steven H. Noll (Reg. 28,982)

SCHIFF, HARDIN LLP
CUSTOMER NO. 26574
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606
Telephone: 312/258-5790
Attorneys for Appellant(s).

CERTIFICATE OF MAILING

I hereby certify this correspondence is being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on December 23, 2005.

Steven H. Noll

STEVEN H. NOLL

CH1\ 4425879.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPELLANT:	Frank Reisinger	CONFIRMATION NO. 4346
SERIAL NO.:	09/340,782	GROUP ART UNIT: 3621
FILED:	June 28, 1999	EXAMINER: Christine O. Sherr
TITLE:	"METHOD FOR THE DEPENDABLE TRANSMISSION SERVICE DATA TO A TERMINAL EQUIPMENT AND ARRANGEMENT FOR IMPLEMENTING THE METHOD"	

MAIL STOP APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPELLANT'S APPEAL BRIEF

S I R:

Pursuant to 37 C.F.R. §41.37, Appellant herewith submits his main Brief in the appeal of the above-referenced application.

REAL PARTY IN INTEREST:

The real party in interest is the assignee of the application, Francotyp-Postalia GmbH, a German corporation, as the successor to the named Assignee of the application, Francotyp-Postalia AG & Co., KG.

RELATED APPEALS AND INTERFERENCES:

There are no related appeals and no related interferences.

STATUS OF CLAIMS:

Claims 1-32 are on appeal, and constitute all of the original claims of the application. No claim has been cancelled during prosecution.

STATUS OF AMENDMENTS:

No Amendment has been filed following the final rejection dated July 27, 2005.

SUMMARY OF THE CLAIMED SUBJECT MATTER:

The method and apparatus of the claims on appeal can be practiced in embodiments as shown in Figure 1a and 1c employing a microprocessor 6 as a control unit, or in an embodiment as shown in Figure 1b, employing a one-time programmable (OTP) processor 6 as the control unit. The basic components and method steps in these different embodiments do not significantly differ, and therefore the embodiment employing a microprocessor will be described below, for simplicity and to avoid duplication.

In general, the method and apparatus which are the subject of the claims on appeal are for the purpose of determining when the contents of a usage memory, wherein usage data are accumulated during the operation of a device, are to be transferred to a remote location for analysis, such as a statistical analysis. Since the primary intended use of the apparatus and method of the claims on appeal is a postage meter, which is a relatively small device having limited memory capacity, the method and apparatus of the claims on appeal make use of monitoring the remaining memory contents of the memory in which the usage data are stored as the criterion for data transfer to the remote location for analysis.

Figure 1a shows a block circuit diagram of the inventive postage meter machine with a printer module 1 for a completely electronically generated franking image. This postage meter machine has at least one input unit 2 with a number of actuation elements, a display unit 3, a modem 23 that produces the communication with a data center. A further input unit 21 and/or a scale 22 is/are coupled to a control unit 6 via an input/output control module 4. The postage meter machine has non-volatile memories 5a, 5b, 9, 10 and 11 for data that contain the variable or the

constant parts of the franking image and programs for processing the data in conjunction with the mail carrier and service to be carried out by the carrier (as explained below). (p.7, l.14-22)

Obtaining the postage fee schedule table data from the data center ensues as needed or in conjunction with the remote loading of the postage meter machine with a credit (postage call for the purpose of re-crediting), with the security measures of the credit loading being utilized also for the table loading. (p.9, l.3-6) The postage fee schedule table data are initially intermediately stored in the memory area 7d of the volatile main memory RAM 7 of the postage meter machine. (p.9, l.6-8) The microprocessor 6 can now form a checksum over the content of the postage fee schedule table data and send this checksum by modem 23 to the data center DZ land-line or radio via a communication network. (p.9, l.8-11) The data center DZ has a modem 33 that is connected to a server 32 that accesses a data bank 31. (p.9, l.11-12) The requesting postage meter machine identifies itself at the data center with its PIN (postage call identification number) and communicates the version number for the purpose of locating a new postage fee schedule table in the data bank DB31 of the data center, wherein a postage fee schedule table is allocated to the communicated version number. (p.9, l.12-16) The server 32 is programmed for checking the proper transmission and error-free intermediate storage of service data on the basis of the checksum, as will be explained in yet greater detail with reference to Figures 3a and 3b. (p.9, l.16-18)

When a modified postage fee schedule table is required in an electronic postage computer, a remote installation can ensue on demand. A postage fee schedule table is to be communicated to the terminal equipment on demand in order

to be able to load this into corresponding memories of the postage computer. (p.10, l.10-13) Given such a remote installation, one embodiment of the inventive method for dependable transmission of service data to a terminal equipment proceeds according to the following method steps:

In step 210 as shown in Fig. 2, new postage fee schedule table data are offered in the data center for a future postage calculation. (p.10, l.13-17) In step 110 the terminal equipment (postage calculator) formulates request data for postage fee schedule table data. (p.10, l.17-18) In a first communication 120 of the terminal equipment with the data center, the request data are transmitted in order to request the new postage fee schedule table data from the data center, and comprising a reception and storing of the requested postage fee schedule table data are subsequently received and stored by the terminal equipment. (p.10, l.18-22) In a first communication 220 of the data center with the terminal equipment, the aforementioned request data are received at the data center and the requested postage fee schedule table data are transmitted to the terminal equipment. (p.10, l.22 - p.11, l.2) In a second communication 130 of the terminal equipment with the data center, a message is formed at the terminal equipment and is communicated to the data center, that refers to the stored, valid, new postage fee schedule table data. (p.11, l.2-5) In a second communication 230 of the data center with the terminal equipment, the aforementioned message is received by and checked in the data center by comparison information generated from the postage fee schedule table data, and an OK message is transmitted to the terminal equipment, and in step 240 a registration of the service performed ensues in the data center in conjunction with the transmission of an OK message. (p.11, l.5-10)

Upon reception of the OK message in the terminal equipment, an indicator that the stored data is registered in valid form ensues and a flag for payment of the service ensues in the data center. As the indicator, either a bit is set in a secured area in the non-volatile memory of the postage computer or corresponding MAC-protected data are stored. The microprocessor only utilizes data registered as valid for calculating postage. (p.11, l.11-16)

The following method steps proceed in an alternative embodiment:

In step 210, new postage fee schedule table data are offered in the data center for a future postage calculation. (p.11, l.17-19) In step 110 the terminal equipment (postage calculator) formulates request data for postage fee schedule table data. (p.11, l.19-20) In a first communication 120 of the terminal equipment with the data center, the request data are transmitted in order to request the new postage fee schedule table data from the data center, and comprising a reception and storing of the requested postage fee schedule table data are subsequently received and stored by the terminal equipment. (p.11, l.19 - p.20, l.1) In a first communication 220 of the data center with the terminal equipment, the aforementioned request data re received at the data center and the requested postage fee schedule table data are transmitted to the terminal equipment. (p.12, l.1-4) In a second communication 130 of the terminal equipment with the data center, a message is formed at the terminal equipment and is communicated to the data center, that refers to the stored, valid, new postage fee schedule table data. (p.12, l. 4-7) In a second communication 230 of the data center with the terminal equipment, the aforementioned message is received by and checked in the data center by comparison information generated from the postage fee schedule table

data, and an OK message is transmitted to the terminal equipment, and in step 240 a registration of the service performed ensues in the data center in conjunction with the transmission of an OK message. (p.12, l. 7-12)

In a second communication 230 of the data center with the terminal equipment, the aforementioned message is received by and checked in the data center by comparison information generated from the postage fee schedule table data, and a load instruction is transmitted to the terminal equipment to load the new postage fee schedule table data into a non-volatile memory of its postage computer. (p.12, l. 13-17)

A registration (step 240) of the loading ensues in the data center, and loading (step 140) of the postage fee schedule table data into a non-volatile memory of the postage computer ensues after reception of the load instruction. (p.12, l. 18-20)

Figures 3a and 3b show first and second versions of a flowchart for checking the dependable transmission of data to the terminal equipment. (p.17, l.8-9)

In one version, shown in Figure 3a, the encrypted checksum is formed by the postage computer on the basis of an asymmetrical encryption algorithm, a public key being stored therein, and an appertaining, private, secret key (PRIVATE KEY) is employed for checking in the data center, this being stored in a secure manner and being kept secret from third parties. (p.17, l.10-14) Given an RSA signature, a message based on the version number and on the checksum is encrypted with a public write key (PUBLIC KEY) to form a digital signature. (p.17, l.14-16) The digital signature (SIGNATURE) is sent from the terminal equipment to the data center together with the identification number PIN and the version number (VERSION NO), the data center being capable of decrypting the signature with a secret read key

(PRIVATE KEY) according to the asymmetrical algorithm (RSA). (p.17, l.16-20) The checksum (CHECK SUM) over the content of the fee schedule table data that are stored in the data bank 31 allocated to the version number (and possibly also allocated to the PIN) must agree with the decrypted message if the fee schedule table data intermediately stored in the postage computer or in the postage meter machine are to be recognized as being valid. (p.17, l.20 - p.18, l.1) This verification is a prerequisite in order to communicate a corresponding command to the postage meter machine. (p.18, l.1-2) The rate table check sum formation can ensue before or during the communication. (p.18, l.3) A prior formation has the advantage that the comparison check sum RATE TABLE CHECK SUM is stored in the data bank 31 allocated to the version number VERSION NO. or PIN and can be called directly from the data bank 31 by the server 32 for comparison. (p.18, l.3-7) The calculating time of the server 32 that is saved is thus advantageously available to the decryption procedure of the SIGNATURE. (p.18, l.7-8) The decrypted message is identical to the checksum CHECK SUM that was formed in the postage computer or terminal equipment from the volatilely intermediately stored postage fee schedule table. (p.18, l.8-10) Given proper intermediate storage, the decrypted checksum CHECK SUM is identical to the comparison checksum RATE TABLE CHECK SUM that is formed or stored in the data bank 31. (p.18, l.11-13)

In another version, shown in Figure 3b, an encrypted checksum MAC (message authentication code) is formed with a symmetrical encryption algorithm, this being formed by the postage meter machine in which a secret key is stored. (p.18, l.18-20) The encrypted checksum MAC is communicated to the data center. (p.18, l.20-21)Differing from the version shown in Figure 3a, no decryption is

implemented in the data center; rather, an encryption is implemented in order to encrypt a checksum derived from the postage fee schedule table to form a comparison MAC=. (p.18, l.21 - p.19, l.1) The RATE TABLE CHECK SUM formation can ensue before or during the communication. Such a prior formation has the advantage that the CHECK SUM merely has to be called from the data bank 31 in order to generate the comparison MAC= from this CHECK SUM by encryption with a secret key SECRET KEY using a symmetrical algorithm DES with the assistance of the server 32. (p.19, l.2-5)

The same secret key SECRET KEY is employed in the check in the data center as in the postage meter machine. (p.19, l.6-7) The check in the data center preferably ensues with both MACs. (p.19, l.7-8) A suitable version of the DES algorithm is preferably utilized in the MAC formation. (p.19, l.8-9) The same secret DES key is employed given a MAC formation in the data center and in the postage meter machine. (p.19, l.9-10) To that end, the secret DES key must be stored secured in the data bank 31 allocated to that PIN identifying the terminal equipment. (p.19, l.10-12) Alternatively, the RATE TABLE CHECK SUM formation and the encryption to form a comparison MAC can ensue in common before the communication. (p.19, l.12-13) The comparison MAC is then stored in the data bank 31 allocated to the PIN and to the version number and can be called by the server for comparison purposes. (p.19, l.13-15)

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL:

The following issues are presented for review in the present Appeal, presented in the manner formulated by the Examiner:

Whether the subject matter of claims 1-11 is anticipated under 35 U.S.C. §102(b) by United States Patent No. 4,802,218 (Wright et al.);

Whether the subject matter of claims 12-16 is anticipated under 35 U.S.C. §102(b) by Wright et al.;

Whether the subject matter of claims 17-27 is anticipated under 35 U.S.C. §102(b) by Wright et al.; and

Whether the subject matter of claims 28-32 is anticipated under 35 U.S.C. §102(b) by Wright et al.

ARGUMENT:

Although all claims of the application stand rejected as being anticipated by Wright et al., the Examiner, in the final rejection and in previous Office Actions, separated the claims according to the four independent claims of the application, as claims 1-11, claims 12-16, claims 17-27 and claims 28-32. Even though the Examiner adopted the identical approach for the independent claims for all of the groups of simply repeating the claim language verbatim, and providing the identical citation to the Wright et al. patent with regard to each independent claim, Appellant nevertheless will provide separate sections below for the groups of claims identified by the Examiner. The following introductory comments, however, are applicable to all of these groups.

The present Appeal is a reinstatement of a previous Appeal. Upon the filing of Appellant's previous Appeal Brief, all of the rejections that were the subject of the original appeal were withdrawn, and the aforementioned rejection based on Wright et al. was made. The Examiner has never undertaken a step-by-step comparison of the steps of the method claims on Appeal against the teachings of the Wright et al.

patent, and has not undertaken a component-by-component analysis of the independent apparatus claims with regard to the teachings of the Wright et al. patent. For example, throughout the prosecution, the Examiner has never specifically identified what component of group of components the Examiner considers to correspond to the "data center" that is claimed in each of the independent claims. Appellant has assumed that the Examiner is equating the card MPU60 in the Wright et al. with the claimed "data center," since that is the only source of data that are to be entered into the terminal in the Wright et al. reference, but the Examiner has never confirmed whether this assumption is correct and in response to that assumption being stated in writing numerous times during prosecution, the Examiner has provided no further information on this point.

Moreover, a central issue throughout prosecution, after prosecution was reopened and the rejection on the Wright et al. reference was made, has been where, in the Wright et al. reference, the Examiner considers a communication to take place between devices or components that are located remotely from each other, as required in each of the independent claims. This issue was the central point argued in Appellant's response to the first Office Action that was issued after prosecution was reopened, and in the final rejection the Examiner, in response to those arguments, provided further citations to the Wright et al. reference. Following the final rejection, an interview was conducted wherein it was explained why none of those further citations has anything to do with a data center and terminal equipment that are remotely-located relative to each other. Now, *for the first time,* in an Advisory Action rendered following Appellant's response to the final rejection, the Examiner has provided another citation to a passage in the Wright et al. reference,

which has never before been cited or relied upon by the Examiner. Presumably, in the Examiner's Answer, the Examiner will have to be more informative and, for the first time, identify components in the Wright et al. reference that the Examiner contends correspond to terminal equipment and a data center that is remotely located relative to the terminal equipment. Of course, this will necessitate the filing of a Reply Brief by the Appellant, since this will be the first time that Appellant will be informed of that position of the Examiner. Appellant respectfully submits that neither the Appellant nor the Board of Patent Appeals and Interferences is well served by having to wait until the Examiner's Answer is filed to learn highly relevant details of the Examiner's position. Moreover, it is inexplicable that the Examiner would wait until rendering an Advisory Action, following the filing of a response to the final rejection, to provide a citation for the first time with respect to an issue that has been central as to whether the Wright et al. reference anticipates the claims on appeal.

REJECTION OF CLAIMS 1-11 AS BEING ANTICIPATED BY WRIGHT ET AL.

As noted above, claim 1 refers to at least one communication between terminal equipment and a data center, the terminal equipment and the data center being remote from each other. In view of the fact that the Examiner merely provided a general citation to the aforementioned lengthy passage in the Wright et al. reference, it is not clear which component or components in the Wright et al. reference the Examiner is considering as being comparable to a data center that is remote from terminal equipment. Since the only data exchange that is described in the passage of Wright et al. cited by the Examiner is a data exchange between a smart card and a postage meter having a card reader that receives the smart card, Appellant assumes the Examiner is considering the meter to be comparable to the

terminal equipment of the independent claims of the application, and is considering the smart card to somehow be the equivalent of a data center remote from the terminal equipment. Appellant does not disagree that the postage meter described in the Wright et al. reference corresponds to the terminal equipment of the claims of the present application, however, the smart card (data carrier) in the Wright et al. reference clearly has no correspondence whatsoever with a data center remote from the terminal equipment. In order for the smart card and the postage meter in the Wright et al. system to communicate with each other, it is essential that the smart card not be remote from the terminal equipment, but be physically inserted in the terminal equipment. The fact that the smart card can be removed from the terminal equipment is irrelevant, because if and when the smart card is removed from the postage meter in the Wright et al. system, it is impossible for there to be any communication between the smart card and the postage meter. The explicit language of each of the independent claims of the present application requires a communication between the terminal equipment and a remote data center located remote from the terminal equipment, meaning that the communication must occur when the data center and the terminal equipment are remote from each other.

Moreover, the Wright et al. reference itself includes language that clearly distinguishes the smart card (data carrier) disclosed therein from a source of data that is remote from the terminal equipment. As stated in the Wright et al. reference in the paragraph beginning at column 1, line 33, the Wright et al. reference distinguishes the type of equipment disclosed therein (characterized as "point-of-sale (POS) terminals" in column 1, line 17 of Wright et al.) from the type of system to which the present application is directed, namely involving terminal equipment and a

data center remote therefrom. The Wright et al. system is directed to maintaining adequate security for such point-of-sale terminals, and characterizes maintaining such security as being problematic because point-of-sale system "conventionally are passive and do not authenticate themselves or the particular transactions for which they are used. Instead, on-line access through a terminal to a central account system, such as a bank or credit card account records, is required for confirmation of each transaction." (Emphasis added, Wright et al., column 1, lines 37-41).

The explicit language of the Wright et al. reference itself, therefore, states that the use of a card as a data carrier, as described in that reference, is not the same as a communication with a remote data source.

The fact that the Wright et al. reference provides no disclosure whatsoever involving a remote data center communicating with a terminal device is sufficient by itself to preclude the Wright et al. reference from anticipating claim 1 of the present application.

Equally as importantly, the Wright et al. reference, particularly the passage cited by the Examiner, merely refers to a "handshake" procedure by which verification of authentification of the inserted card is accomplished. This type of security verification has nothing to do with the type of data verification to which the subject matter of claim 1 is directed, i.e, to ensure that data have been correctly transferred (downloaded) from the remote data center to the terminal equipment. It is for this reason that in each of the independent claims of the present application, the return or answerback message that proceeds from the terminal equipment to the data center is formed by involving the originally transmitted message itself.

Independent claim 1 states that the answerback message "refers to" the originally transmitted message.

The handshake procedure disclosed in the Wright et al. reference, because it is simply to verify the authenticity or the authorization of the card that is currently inserted in the postage meter, does not involve a transfer of data whereby the correctness of the transfer data needs to be verified. Even though in the Wright et al. reference a serial number is transmitted from the card to the device, and a verification is made based on that serial number and a verification message is then transmitted back to the card to then enable a subsequent further exchange between the card and the postage meter, the message that is transmitted back to the card from the postage meter is simply a "yes" or "no" statement verifying or denying authorization. The message that is transmitted back to the card from the postage meter does not in any way refer to the originally transmitted serial number itself, nor does it include any coded information that has been based on or derived from the originally transmitted serial number.

Moreover, independent claim 1 requires that the verification take place in separate first and second communications. The Examiner did not identify what steps of functions in the cited passage of Wright et al. the Examiner considers as corresponding to these first and second communications. In independent claims 1 and 17, each of the first and second communications includes a transmission in both directions between the data center and the terminal equipment. The aforementioned handshake procedure in the Wright et al. is a single communication between the card and the postage meter. There is no second communication involved in the handshake procedure in the Wright et al. reference. Although a further data

exchange between the card and the postage meter can occur in the Wright et al. system, after verification has been accomplished, this further exchange is not in any way involved in the handshake procedure, and in fact cannot even proceed until the handshake procedure has been completed so that verification has been established.

In response to these arguments, at paragraph 4 on page 2 of the final rejection, the Examiner directed Appellant's attention to column 14, lines 41-60 in the Wright et al reference. Appellant is unable to find any statement whatsoever in that passage that refers to, or could be interpreted as a reference to, a "data center," remote or otherwise.

The aforementioned passage cited by the Examiner refers to the service card being loaded into the terminal MPU30. The terminal MPU30 is the microprocessor that is located in the terminal unit, and can be accessed by the service card (or other data-carrying cards), only by those cards being physically inserted in the terminal equipment. It should be noted that Figure 2a of the Wright et al reference shows the card MPU as a separate block from the terminal 20 and the terminal MPU30, connected thereto by arrowed lines, but these arrowed lines merely schematically indicate the flow of data between the card MPU and the terminal MPU30, via a handshake channel 61, and do not indicate any "remoteness" of the card or the card MPU from the terminal MPU30. This is made explicitly clear in Figure 7 of the Wright et al reference, wherein each card is shown as being inserted in the unit 20', so as to be able to communicate with the terminal MPU30 thereof.

Therefore, there is no data source ("data center" or otherwise) that is located remote from the terminal equipment, as explicitly required in independent claim 1 of the present application. Moreover, there is no component in the Wright et al

reference that corresponds to a "data center" as that term is commonly understood by those of ordinary skill in the relevant technology.

The term "data center" inherently means, or refers to, a center that is remote from the terminal units with which it communicates. Such communication may be wireless or by land lines, but in all instances the data center is located remote from the terminal equipment that it services. This is made clear in the present application by the indication in Figure 1 of the communication between the data center DC and the I/O controller 4 via the modem 23.

This is also consistent with almost every reference that the Examiner has made of record. In United States Patent No. 5,008,827 (Sansone et al), the PB data center 18 (Fig. 1) and the central station 18 (Fig. 4) are clearly remote from the terminal equipment with which they communicate.

In United States Patent No. 6,064,994 (Kubatzki et al), the data central DC is clearly indicated as communicating with a postage meter machine FM via line 17, clearly a remote arrangement.

In United States Patent No. 5,715,164 (Liechti et al), the data center 15 is again shown to communicate wirelessly with postage meters 101-1 through 101-P.

In United States Patent No. 4,752,950 (Le Carpentier), the central station 2 communicates with a telephone network 3 via modems 6V, and the telephone network 3, in turn, communicates with local stations 4X through 4Z respectively via modems 6X through 6Z. Again, a remote arrangement.

The same is true in numerous references cited by the Appellant.

In United States Patent No. 5,699,415 (Wagner), for example, the data center 18 is clearly shown as communicating with the user station 10 via communication

terminal equipment 14 and 16, and communication line 15. Again, a remote arrangement.

The same is true in United States Patent No. 4,097,923 (Eckert, Jr. et al), wherein the blocks 1 represent remote postage meter stations capable of communicating with a data center represented by block 5 (column 5, lines 50-52).

European Application 0 647 925 shows a data center 112 communicating with a so-called "postage evidencing device" 114, again in a remote arrangement.

Hundreds, if not thousands, of other examples could be cited.

It is thus abundantly clear that the term "data center" as used in the claims of the present application inherently means a device that is located remote from the terminal equipment. This, in addition to the aforementioned explicit statements in the preambles of each of the independent claims, clearly precludes the Wright et al reference from reading on any of those claims.

Appellant recognizes that the Examiner is required to give all terms in a patent claim the broadest reasonable interpretation. Appellant submits, however, this does not permit the Examiner to ignore common, well-understood meanings for terms, otherwise every term having a well-understood meaning would have to be re-defined in each patent claim in which it is used. As long as there is nothing in the claim language itself, and nothing in the specification, to indicate that a word having a common, well-understood meaning to those of ordinary skill in the relevant technology is being used in a manner contrary to that well-understood meaning, the well-understood meaning must be accepted, and the claim interpreted according to that well-understood meaning.

Appellant respectfully submits that such is the case in each of the independent claims of the present application. In view of the complete absence anywhere in the Wright et al reference of the use of a "data center" or any equivalent component for entering data into a terminal unit in the manner set forth in the independent claims of the present application, the Wright et al reference does not anticipate claim 1.

In response to these arguments, in the aforementioned Advisory Action (dated October 21, 2005) the Examiner for the first time indicated a citation to column 7, lines 57-62 of the Wright et al. reference. That passage merely states that although the above-described handshake procedure in Wright et al. can be performed with an operation microprocessor for the terminal, or one remote to the terminal, it is preferred that the procedure be performed with a secure microprocessor embedded in the actual value dispensing section of the terminal.

Referring to Figure 2a of the Wright et al. reference, this merely means that the terminal MPU30, instead of being located within the terminal housing 20, could be located outside of that housing, but that has nothing to do with whether the Wright et al. reference discloses a data center that is remote from the terminal equipment, since the Examiner has never contended that the terminal MPU30 corresponds to the claimed "data center." Moreover, the handshake procedure, as described above, does not involve transfer or storage of the actual data to be transmitted from the data center to the terminal equipment, but is only a preliminary procedure that is undertaken to authorize such a transfer in the Wright et al. Therefore, whether the terminal MPU30 is within the housing of the terminal equipment 20 or possibly

remote thereto is completely irrelevant to the applicability of the Wright et al. reference to the language of claim 1.

Claims 2-11 add further method steps to the novel method of claim 1, and are therefore not anticipated by Wright et al. for the same reasons discussed above in connection with claim 1.

REJECTION OF CLAIMS 12-16 AS BEING ANTICIPATED UNDER §102(b) BY WRIGHT ET AL.

Since the Examiner applied the same citations from Wright et al. against independent claim 12 as were applied against independent claim 1, Appellant's argument above with regard to independent claim 1 are equally applicable to claim 12. Claims 13-16 add further steps the novel method of claim 12, and are therefore not anticipated by Wright et al. for the same reasons as to why claim 12 is not anticipated by Wright et al.

REJECTION OF CLAIMS 17-27 AS BEING ANTICIPATED UNDER §102(b) BY WRIGHT ET AL.

Since the Examiner applied the same citations from Wright et al. against independent claim 17 as were applied against independent claim 1, Appellant's argument above with regard to independent claim 1 are equally applicable to claim 17. Claims 18-27 add further steps the novel apparatus of claim 17, and are therefore not anticipated by Wright et al. for the same reasons as to why claim 17 is not anticipated by Wright et al.

REJECTION OF CLAIMS 28-32 AS BEING ANTICIPATED UNDER §102(b) BY WRIGHT ET AL.

Since the Examiner applied the same citations from Wright et al. against independent claim 28 as were applied against independent claim 1, Appellant's argument above with regard to independent claim 1 are equally applicable to claim

28. Claims 29-32 add further steps the novel apparatus of claim 28, and are therefore not anticipated by Wright et al. for the same reasons as to why claim 28 is not anticipated by Wright et al.

CONCLUSION:

For the above reasons, Appellant respectfully submits the Examiner is in error in law and in fact in rejecting claims 1-32. Reversal of these rejections is proper, the same is respectfully requested.

Submitted by,

Steven H. Noll (Reg. 28,982)

SCHIFF, HARDIN LLP
CUSTOMER NO. 26574
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606
Telephone: 312/258-5790
Attorneys for Appellant.

APPENDIX "A"

1. A method for dependably transmitting service data from a data center to remotely-located terminal equipment, comprising the steps of:

offering new service data at a data center for future use at terminal equipment;

forming a request for new service data at the terminal equipment;

establishing a first communication between the terminal equipment and the data center and in said first communication transmitting said request data from the terminal equipment to the data center, receiving the request data at the data center, transmitting the new service data requested in the request data from the data center to the terminal equipment, and receiving and storing the new service data at the terminal equipment; and

establishing a second communication between the terminal equipment and the data center and in said second communication forming a message at the terminal equipment that refers to the new service data stored at the terminal equipment, communicating said message from the terminal equipment to the data center, receiving the message from the terminal equipment at the data center and checking the message at the data center by comparison of information contained in the message with information generated from the new service data at the data center and, given a positive comparison result, transmitting a follow-up message from the data center to the terminal equipment allowing said

terminal equipment, when appropriate, to use said new service data, and registering at the data center the valid transmission of the new service data to the terminal equipment.

2. A method as claimed in claim 1 wherein said follow-up message comprises an OK message allowing the terminal equipment to be switched into an operating mode.

3. A method as claimed in claim 2 wherein the step of transmitting said OK message includes transmitting a marking in said OK message indicating that the new service data stored at the terminal equipment are valid.

4. A method as claimed in claim 1 wherein the step of storing the new service data in the first communication comprises intermediately storing the new service data at the terminal equipment, and wherein the step of transmitting said follow-up message in said second communication comprises transmitting a load instruction from the data center to the terminal equipment, and wherein said second communication includes the step of, upon receipt of said load instruction at the terminal equipment, loading the new service data into a non-volatile memory of a processing module at the terminal equipment.

5. A method as claimed in claim 1 wherein the step of forming said message in the second communication at the terminal equipment comprises forming a message including a version number associated with the new service data and a checksum.

6. A method as claimed in claim 1 wherein the step of forming said message in the second communication at the terminal equipment comprises forming

a message including a version number associated with the new service data and an encrypted checksum.

7. A method as claimed in claim 1 wherein the step of offering said new service data comprises offering postage fee schedule table data as said new service data, and comprising the step of providing a postage computer having a processing module which makes use of said postage fee schedule table data at said terminal equipment.

8. A method as claimed in claim 7 wherein the step of forming said message in said second communication at said terminal equipment includes forming a message including a version number of the new service data and an encrypted checksum, and comprising the step of providing a postage meter machine at said terminal equipment in communication with said postage computer, storing a secret key in said postage meter machine, forming said encrypted checksum in said postage meter machine using a symmetrical encryption algorithm and said secret key, and storing said secret key as well at said data center and using said secret key at said data center to check said message from said terminal equipment in said second communication.

9. A method as claimed in claim 7 wherein the step of forming said message in said second communication at said terminal equipment comprises forming a message including a version number of the new service data and an encrypted checksum, and comprising the steps of storing a public key in said postage computer and forming said encrypted checksum in said postage computer using an asymmetrical encryption algorithm and said public key, and storing a non-public secret key, related to said public key, at said data center and using said non-

public secret key at said data center to check said message in said second communication.

10. A method as claimed in claim 1 wherein the step of offering new service data at said data center comprises offering new postage fee schedule table data at said data center for future use in postage calculation, and wherein the step of checking the message transmitted from the terminal equipment to the data center in the second communication comprises checking information contained in said message by comparison with information generated from the new postage fee schedule table data, and wherein the step of transmitting said follow-up message in said second communication from said data center to the terminal equipment comprises transmitting an OK message indicating that the new postage fee schedule table data received at said terminal equipment are valid and also including a load instruction instructing the terminal equipment to load the new postage fee schedule table data into a non-volatile memory of a postage computer at said terminal equipment.

11. A method as claimed in claim 10 comprising the additional step of loading said new postage fee schedule table data into said non-volatile memory at said postage computer upon receipt at said terminal equipment of said follow-up message.

12. A method for dependably transmitting service data from a data center to remotely-located terminal equipment, comprising the steps of:

transmitting unencrypted service data from a data center to terminal equipment;

generating a code at the terminal equipment based on the transmitted service data;

transmitting said code from said terminal equipment to said data center; and

receiving said code at said data center and checking said code at said data center and transmitting a message from said data center to said terminal equipment identifying a result of the check.

13. A method as claimed in claim 12 comprising providing a postage computer at said terminal equipment, and wherein the step of transmitting unencrypted service data to the terminal equipment comprises transmitting unencrypted fee schedule table data, as said unencrypted service data, to said postage computer, and comprising the steps of generating a checksum at said postage computer based on the transmitted fee schedule table data and transmitting the checksum to the data center as at least a part of said code, and wherein the step of checking the code at the data center comprises checking the checksum at the data center on the basis of a stored checksum stored at said data center and wherein the step of transmitting a message to the terminal equipment comprises transmitting an OK message to the terminal equipment given coincidence of said stored checksum with the checksum transmitted to the data center.

14. A method as claimed in claim 12 comprising providing a postage computer at said terminal equipment, and wherein the step of transmitting unencrypted service data to the terminal equipment comprises transmitting unencrypted fee schedule table data, as said unencrypted service data, to said postage computer, and comprising the steps of generating a encrypted code at said postage computer based on the transmitted fee schedule table data and transmitting

the encrypted code to the data center as at least a part of said code, and wherein the step of checking the code at the data center comprises checking the encrypted code at the data center on the basis of a stored encrypted code stored at said data center and wherein the step of transmitting a message to the terminal equipment comprises transmitting an OK message to the terminal equipment given coincidence of said stored encrypted code with the encrypted code transmitted to the data center.

15. A method as claimed in claim 12 comprising providing a postage computer at said terminal equipment and wherein the step of transmitting unencrypted service data to the terminal equipment comprises transmitting unencrypted fee schedule table data, as said unencrypted service data, to said postage computer, and wherein the step of generating a code at the terminal equipment comprises generating a signature representing information dependent on the transmitted fee schedule table data and encrypting said information with a public write key to form said signature, and wherein the step of transmitting said code to the data center comprises transmitting said signature to the data center, and wherein the step of checking the code at the data center comprises decrypting the signature at the data center with a secret read key according to an asymmetrical algorithm and checking the information in the signature with information stored at the data center and, given a positive comparison result, transmitting an OK message to the terminal equipment.

16. A method as claimed in claim 15 comprising the step of forming a checksum as said information contained in said signature.

17. An arrangement for dependably transmitting service data from a data center to remotely-located terminal equipment, comprising:

a data center, and terminal equipment located remote from said data center, said data center offering new service data for future use at said terminal equipment;

means for forming a request for new service data at the terminal equipment;

means for establishing a first communication between the terminal equipment and the data center and in said first communication transmitting said request data from the terminal equipment to the data center, means for receiving the request data at the data center and for transmitting the new service data requested in the request data from the data center to the terminal equipment, and means for receiving and storing the new service data at the terminal equipment; and

means for establishing a second communication between the terminal equipment and the data center and in said second communication forming a message at the terminal equipment that refers to the new service data stored at the terminal equipment and for communicating said message from the terminal equipment to the data center, means for receiving the message from the terminal equipment at the data center and for checking the message at the data center by comparing information contained in the message with information generated from the new service data at the data center and, given a positive comparison result, for forming and transmitting a follow-up message from the data center to the terminal equipment allowing said terminal equipment, when appropriate, to use said new service data, and

means for registering at the data center the valid transmission of the new service data to the terminal equipment.

18. An arrangement as claimed in claim 17 wherein said means for forming said follow-up message comprises means for forming an OK message allowing the terminal equipment to be switched into an operating mode.

19. An arrangement as claimed in claim 18 wherein said means for forming said OK message means for including a marking in said OK message indicating that the new service data stored at the terminal equipment are valid.

20. An arrangement as claimed in claim 17 wherein said means for storing the new service data in the first communication comprise means for intermediately storing the new service data at the terminal equipment, and wherein said means for transmitting said follow-up message in said second communication comprise means for transmitting a load instruction from the data center to the terminal equipment, and wherein said terminal equipment comprises means for, upon receipt of said load instruction at the terminal equipment, loading the new service data into a non-volatile memory of a processing module at the terminal equipment.

21. An arrangement as claimed in claim 17 wherein said means for forming said message in the second communication at the terminal equipment comprise means for forming a message including a version number associated with the new service data and a checksum.

22. An arrangement as claimed in claim 17 wherein said means for forming said message in the second communication at the terminal equipment comprise means for forming a message including a version number associated with the new service data and an encrypted checksum.

23. An arrangement as claimed in claim 17 wherein said data center comprises means for offering postage fee schedule table data as said new service data, and wherein said terminal equipment comprises a postage computer having a processing module which makes use of said postage fee schedule table data.

24. An arrangement as claimed in claim 23 wherein said means for forming said message in said second communication at said terminal equipment comprise means for forming a message including a version number of the new service data and an encrypted checksum, and wherein said terminal equipment comprises a postage meter machine in communication with said postage computer, means for storing a secret key in said postage meter machine, means for forming said encrypted checksum in said postage meter machine using a symmetrical encryption algorithm and said secret key, and wherein said data center comprises means for storing said secret key as well at said data center and wherein said means for checking comprise means for using said secret key to check said message from said terminal equipment in said second communication.

25. An arrangement as claimed in claim 23 wherein said means for forming said message in said second communication at said terminal equipment comprise means for forming a message including a version number of the new service data and an encrypted checksum, and wherein said postage computer comprises means for storing a public key and for forming said encrypted checksum using an asymmetrical encryption algorithm and said public key, and wherein said data center comprises means for storing a non-public secret key, related to said public key, at said data center and wherein said means for checking comprise means for using said non-public secret key to check said message in said second communication.

26. An arrangement as claimed in claim 17 wherein said data center comprises means for offering new postage fee schedule table data at said data center for future use in postage calculation, and wherein said means for checking the message transmitted from the terminal equipment to the data center in the second communication comprises means for checking information contained in said message by comparison with information generated from the new postage fee schedule table data, and wherein said means for transmitting said follow-up message in said second communication from said data center to the terminal equipment comprises means for transmitting an OK message indicating that the new postage fee schedule table data received at said terminal equipment are valid and also including a load instruction instructing the terminal equipment to load the new postage fee schedule table data into a non-volatile memory of a postage computer at said terminal equipment.

27. An arrangement as claimed in claim 26 wherein said terminal equipment comprises loading said new postage fee schedule table data into said non-volatile memory at said postage computer upon receipt at said terminal equipment of said follow-up message.

28. An arrangement for dependably transmitting service data from a data center to remotely-located terminal equipment, comprising:

a data center, and terminal equipment located remote from said data center;

means for transmitting unencrypted service data from the data center to the terminal equipment;

means for generating a code at the terminal equipment based on the transmitted service data;

means for transmitting said code from said terminal equipment to said data center; and

means for receiving said code at said data center and for checking said code at said data center and for transmitting a message from said data center to said terminal equipment identifying a result of the check.

29. An arrangement as claimed in claim 28 wherein said terminal equipment comprises a postage computer, and wherein said means for transmitting unencrypted service data to the terminal equipment comprises means for transmitting unencrypted fee schedule table data, as said unencrypted service data, to said postage computer, and wherein said postage computer comprises means for generating a checksum based on the transmitted fee schedule table data and wherein said means for transmitting said code comprise means for transmitting the checksum to the data center as at least a part of said code, and said means for checking the code at the data center comprise means for checking the checksum at the data center on the basis of a stored checksum stored at said data center and for transmitting a message to the terminal equipment comprising an OK message to the terminal equipment given coincidence of said stored checksum with the checksum transmitted to the data center.

30. An arrangement as claimed in claim 28 wherein said terminal equipment comprises a postage computer, and said means for transmitting unencrypted service data to the terminal equipment comprises means for transmitting unencrypted fee schedule table data, as said unencrypted service data, to said postage computer, and wherein said postage computer comprises means for generating a encrypted code based on the transmitted fee schedule table data and

wherein said means for transmitting said code comprise means for transmitting the encrypted code to the data center as at least a part of said code, and wherein said means for checking the code at the data center comprise means for checking the encrypted code at the data center on the basis of a stored encrypted code stored at said data center and for transmitting a message to the terminal equipment comprising an OK message to the terminal equipment given coincidence of said stored encrypted code with the encrypted code transmitted to the data center.

31. An arrangement as claimed in claim 28 wherein said terminal equipment comprises a postage computer and wherein said means for transmitting unencrypted service data to the terminal equipment comprise means for transmitting unencrypted fee schedule table data, as said unencrypted service data, to said postage computer, and wherein said postage computer comprises said means for generating a code at the terminal equipment, said postage computer generating a signature, as said code, representing information dependent on the transmitted fee schedule table data and encrypting said information with a public write key to form said signature, and wherein said means for transmitting said code to the data center comprises means for transmitting said signature to the data center, and said means for checking the code at the data center comprise means for decrypting the signature at the data center with a secret read key according to an asymmetrical algorithm and for checking the information in the signature with information stored at the data center and, given a positive comparison result, for transmitting an OK message to the terminal equipment.

32. An arrangement as claimed in claim 31 wherein said postage computer comprises forming a checksum as said information contained in said signature.